Computing rational points on databases of genus 3 curves

Sachi Hashimoto
joint with María de Frutos Fernández and Travis Morrison

Boston University

AMS Graduate Student Conference in Algebraic Geometry and Number Theory at Brown
April 16, 2019
Set-up

A curve $X$ is the solution to a polynomial in two variables $f(x, y) = 0$ with coefficients in $\mathbb{Q}$. 

Curves are classified by their genus: Faltings's theorem (1983) states that a curve $X$ of genus $g \geq 2$ has finitely many rational points; but, it does not give an explicit recipe to compute $X(\mathbb{Q})$. 

Databases of rational points Sachi Hashimoto
Set-up

A curve $X$ is the solution to a polynomial in two variables $f(x, y) = 0$ with coefficients in $\mathbb{Q}$. Solutions $(x, y)$ with rational coordinates are *rational points* on the curve, $X(\mathbb{Q})$ is the set of all such points.
A curve \( X \) is the solution to a polynomial in two variables \( f(x, y) = 0 \) with coefficients in \( \mathbb{Q} \). Solutions \((x, y)\) with rational coordinates are \textit{rational points} on the curve, \( X(\mathbb{Q}) \) is the set of all such points.

Curves are classified by their genus:

\[ g = 0 \quad g = 1 \quad g = 2 \]

- \( g = 0 \): \( \# X(\mathbb{Q}) \) can be \( \infty \)
- \( g = 1 \): \( \# X(\mathbb{Q}) \) can be \( \infty \) always
- \( g = 2 \): \( \# X(\mathbb{Q}) < \infty \) always

Faltings’s theorem (1983) states that a curve \( X \) of genus \( g \geq 2 \) has finitely many rational points; but, it does not give an explicit recipe to compute \( X(\mathbb{Q}) \).
Motivating question

Problem (Motivating question)

Given a curve $X$ of genus $g \geq 2$, can we compute $X(\mathbb{Q})$?
Motivating question

Problem (Motivating question)

Given a curve $X$ of genus $g \geq 2$, can we compute $X(\mathbb{Q})$?

Diophantus (3rd century AD) published over 100 equations and numerical solutions. A genus 2 equation in Diophantus’s books was not solved until 1998 by Wetherell.
We will focus on Chabauty-Coleman method, a (modern interpretation) of an early attempt at proof of Faltings’s theorem. Proves finiteness of $X(\mathbb{Q})$ for curves with Mordell-Weil rank $r$ strictly less than their genus $g$. 
We will focus on Chabauty-Coleman method, a (modern interpretation) of an early attempt at proof of Faltings’s theorem. Proves finiteness of $X(\mathbb{Q})$ for curves with Mordell-Weil rank $r$ strictly less than their genus $g$.

A curve $X$ embeds into its Jacobian $J$, an abelian variety. The Mordell-Weil theorem proves $J(\mathbb{Q})$ is a finitely generated abelian group, thus $J(\mathbb{Q}) \cong \mathbb{Z}^r \oplus J(\mathbb{Q})_{\text{tors}}$. We call $r$ the rank of the curve.
Examples

The “Cursed” Curve, the (non)split Cartan modular curve of level 13, has 7 rational points (Balakrishnan, Dogra, Müller, Tuitman, Vonk).

\[y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z - 32x^2z^2 - 40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 - 16z^4\]
Examples

The “Cursed” Curve, the (non)split Cartan modular curve of level 13, has 7 rational points (Balakrishnan, Dogra, Müller, Tuitman, Vonk).

\[ y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z - 32x^2z^2 - 40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 \]
Examples

The “Cursed” Curve, the (non)spli t Cartan modular curve of level 13, has 7 rational points (Balakrishnan, Dogra, Müller, Tuitman, Vonk).

\[ y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z - 32x^2z^2 - 40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 \]

Relates to Serre’s open image problem, and develops explicit side of Minhyong Kim’s nonabelian Chabauty program.
Examples

The curve $x^4 + y^4 = 17z^4$ has only the rational points $(\pm 1, \pm 2, 1), (\pm 2, \pm 1, 1)$ (Flynn, Wetherell).
The curve $x^4 + y^4 = 17z^4$ has only the rational points $(\pm 1, \pm 2, 1), (\pm 2, \pm 1, 1)$ (Flynn, Wetherell).

This is a genus 3 rank 6 curve which maps to two different elliptic curves of rank 2. It has a cover by a genus 2 rank 2 curve.
The curve $x^4 + y^4 = 17z^4$ has only the rational points $(\pm 1, \pm 2, 1), (\pm 2, \pm 1, 1)$ (Flynn, Wetherell).

This is a genus 3 rank 6 curve which maps to two different elliptic curves of rank 2. It has a cover by a genus 2 rank 2 curve.

Serre posed this problem *Lectures on the Mordell-Weil Theorem*. 
• If \(X(\mathbb{Q})\) is contained in a finite computable set \(X(\mathbb{Q}_p)_1\) then we can compute \(X(\mathbb{Q})\) plus an extra bit, and hope the extra bit is not too big.

• If we can bound the size of \(X(\mathbb{Q})\) then with some luck the bound is often correct.
We are interested in the embedding of our curve $X$ inside of its Jacobian $J$. 

Genus 2 curve embedding into Kummer surface
Big idea

We are interested in the embedding of our curve $X$ inside of its Jacobian $J$.

On $J(\mathbb{Q}_p)$ we will define functionals $f_i$ which are zero on $X(\mathbb{Q})$ but not identically zero, and have finitely many zeros.
Coleman integration

$X/\mathbb{Q}$ a curve, $P, Q, R \in X(\mathbb{Q}_p)$, $\omega, \omega'$ holomorphic 1-forms. Coleman defined an integral $\int_P^Q \omega$. 

• A curve decomposes into residue discs, preimages of points of $X(\mathbb{F}_p)$. Integration inside a single disc is straightforward.

• Integrating between discs happens by "analytic continuation along the Frobenius".

• Satisfies the properties:

1. Linearity: $\int_P^Q (\alpha \omega + \beta \omega') = \alpha \int_P^Q \omega + \beta \int_P^Q \omega'$.

2. Additivity: $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$.

3. Change of variables: if $X'$ is a curve and $\phi: X \rightarrow X'$ a rigid analytic map between wide opens then $\int_P^Q \phi^* \omega = \int_{\phi(Q)}^{\phi(P)} \omega$.

For example, $\phi$ can be taken to be a lift of the $p$th power Frobenius.

4. Fundamental theorem of calculus: $\int_P^Q df = f(Q) - f(P)$. 

Databases of rational points Sachi Hashimoto 9
Coleman integration

$X/\mathbb{Q}$ a curve, $P, Q, R \in X(\mathbb{Q}_p)$, $\omega, \omega'$ holomorphic 1-forms.

Coleman defined an integral $\int_P^Q \omega$.

- A curve decomposes into residue discs, preimages of points of $X(\mathbb{F}_p)$. Integration inside a single disc is straightforward.
Coleman integration

$X/\mathbb{Q}$ a curve, $P, Q, R \in X(\mathbb{Q}_p)$, $\omega, \omega'$ holomorphic 1-forms. Coleman defined an integral $\int_P^Q \omega$.

- A curve decomposes into residue discs, preimages of points of $X(\mathbb{F}_p)$. Integration inside a single disc is straightforward.
- Integrating between discs happens by “analytic continuation along the Frobenius”.

For example, $\phi$ can be taken to be a lift of the $p$th power $\text{Frob}_p$. 

Fundamental theorem of calculus: $\int_P^Q \omega = f(Q) - f(P)$. 

Databases of rational points Sachi Hashimoto 9
Coleman integration

$X/\mathbb{Q}$ a curve, $P, Q, R \in X(\mathbb{Q}_p)$, $\omega, \omega'$ holomorphic 1-forms.

Coleman defined an integral $\int_P^Q \omega$.

- A curve decomposes into residue discs, preimages of points of $X(\mathbb{F}_p)$. Integration inside a single disc is straightforward.
- Integrating between discs happens by “analytic continuation along the Frobenius”.
- Satisfies the properties:

  1. Linearity: $\int_P^Q (\alpha \omega + \beta \omega') = \alpha \int_P^Q \omega + \beta \int_P^Q \omega'$.
  2. Additivity: $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$.
  3. Change of variables: if $X'$ is a curve and $\phi: X \to X'$ a rigid analytic map between wide opens then
     $\int_P^Q \phi^* \omega = \int_{\phi(P)}^{\phi(Q)} \omega$.
     For example, $\phi$ can be taken to be a lift of the $p$th power Frobenius.
  4. Fundamental theorem of calculus: $\int_P^Q df = f(Q) - f(P)$.
Coleman integration

$X/\mathbb{Q}$ a curve, $P, Q, R \in X(\mathbb{Q}_p)$, $\omega, \omega'$ holomorphic 1-forms.

Coleman defined an integral $\int^Q_P \omega$.

- A curve decomposes into residue discs, preimages of points of $X(\mathbb{F}_p)$. Integration inside a single disc is straightforward.
- Integrating between discs happens by "analytic continuation along the Frobenius".
- Satisfies the properties:
  1. Linearity: $\int^Q_P (\alpha \omega + \beta \omega') = \alpha \int^Q_P \omega + \beta \int^Q_P \omega'$. 

Databases of rational points Sachi Hashimoto 9
Coleman integration

$X/\mathbb{Q}$ a curve, $P, Q, R \in X(\mathbb{Q}_p)$, $\omega, \omega'$ holomorphic 1-forms.

Coleman defined an integral $\int_P^Q \omega$.

- A curve decomposes into residue discs, preimages of points of $X(\mathbb{F}_p)$. Integration inside a single disc is straightforward.
- Integrating between discs happens by “analytic continuation along the Frobenius”.
- Satisfies the properties:
  1. Linearity: $\int_P^Q (\alpha \omega + \beta \omega') = \alpha \int_P^Q \omega + \beta \int_P^Q \omega'$.
  2. Additivity: $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$. 
Coleman integration

$X/\mathbb{Q}$ a curve, $P, Q, R \in X(\mathbb{Q}_p)$, $\omega, \omega'$ holomorphic 1-forms.

Coleman defined an integral $\int_P^Q \omega$.

- A curve decomposes into residue discs, preimages of points of $X(\mathbb{F}_p)$. Integration inside a single disc is straightforward.
- Integrating between discs happens by “analytic continuation along the Frobenius”.
- Satisfies the properties:
  1. Linearity: $\int_P^Q (\alpha \omega + \beta \omega') = \alpha \int_P^Q \omega + \beta \int_P^Q \omega'$.
  2. Additivity: $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$.
  3. Change of variables: if $X'$ is a curve and $\phi : X \to X'$ a rigid analytic map between wide opens then $\int_P^Q \phi^* \omega = \int_{\phi(P)}^{\phi(Q)} \omega$.

For example, $\phi$ can be taken to be a lift of the $p$th power Frobenius.
Coleman integration

$X/\mathbb{Q}$ a curve, $P, Q, R \in X(\mathbb{Q}_p)$, $\omega, \omega'$ holomorphic 1-forms.

Coleman defined an integral $\int_P^Q \omega$.

- A curve decomposes into residue discs, preimages of points of $X(\mathbb{F}_p)$. Integration inside a single disc is straightforward.
- Integrating between discs happens by “analytic continuation along the Frobenius”.
- Satisfies the properties:
  1. Linearity: $\int_P^Q (\alpha \omega + \beta \omega') = \alpha \int_P^Q \omega + \beta \int_P^Q \omega'$.
  2. Additivity: $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$.
  3. Change of variables: if $X'$ is a curve and $\phi : X \to X'$ a rigid analytic map between wide opens then $\int_P^Q \phi^* \omega = \int_{\phi(P)}^{\phi(Q)} \omega$. For example, $\phi$ can be taken to be a lift of the $p$th power Frobenius.
  4. Fundamental theorem of calculus: $\int_P^Q df = f(Q) - f(P)$.
$J_{\mathbb{Q}_p}$ is a $p$-adic Lie group, $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ is a $g$-dimensional $\mathbb{Q}_p$-vector space with basis $\omega_i$ which restricts to $X_{\mathbb{Q}_p}$. For example: $x^i dx/y$ is a basis for a hyperelliptic curve.
$J_{\mathbb{Q}_p}$ is a $p$-adic Lie group, $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ is a $g$-dimensional $\mathbb{Q}_p$-vector space with basis $\omega_i$ which restricts to $X_{\mathbb{Q}_p}$. For example: $x^i dx/y$ is a basis for a hyperelliptic curve.

These $\omega_i$ are translation invariant. Locally, we have a map

$log : J(\mathbb{Q}_p) \rightarrow H^0(J_{\mathbb{Q}_p}, \Omega^1)^* \text{ given by } P \mapsto (\omega_i \mapsto \int_b^P \omega_i).$
Fixing $b \in X(\mathbb{Q})$ fixes an embedding $X \hookrightarrow J$. Define $g$ linear functionals

$$f_i : \int_b^z \omega_i : X(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p$$
Fixing $b \in X(\mathbb{Q})$ fixes an embedding $X \hookrightarrow J$. Define $g$ linear functionals

$$f_i : \int_b^z \omega_i : X(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p$$

When rank $r$ of $J(\mathbb{Q})$ is less than the genus, then $\overline{J(\mathbb{Q})}$ is a $\mathbb{Z}_p$-module of rank $r' \leq r$, so functionals must satisfy $g - r'$ relations on (the finite set) $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \supseteq X(\mathbb{Q})$.
Fixing \( b \in X(\mathbb{Q}) \) fixes an embedding \( X \hookrightarrow J \). Define \( g \) linear functionals

\[
    f_i : \int_b^z \omega_i : X(\mathbb{Q}_p) \to \mathbb{Q}_p
\]

When rank \( r \) of \( J(\mathbb{Q}) \) is less than the genus, then \( \overline{J(\mathbb{Q})} \) is a \( \mathbb{Z}_p \)-module of rank \( r' \leq r \), so functionals must satisfy \( g - r' \) relations on (the finite set) \( X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \supseteq X(\mathbb{Q}) \).

\[
    X(\mathbb{Q}_p)_1 := \left\{ z \in X(\mathbb{Q}_p) : \lambda_i \int_b^z \omega_i = 0 \text{ for all } g - r' \text{ relations } \lambda \right\}
\]
Remark

The functions $f_i$ are locally analytic functions, and so $X(\mathbb{Q}_p)_1$, and thus $X(\mathbb{Q})$ is finite.
Remark

The functions $f_i$ are locally analytic functions, and so $X(Q_p)_1$, and thus $X(Q)$ is finite.

Within a residue disc, an integral $\int_{P'} \omega = \int_{P(t)}^{P'(t)} \omega(t) dt$ has a power series expansion in a uniformizer $t$. 

Bound number of zeros with Newton polygon.

Global bound: if $p > 2g$, then $\# X(Q) \leq \# X(F_p) + (2g - 2)$.

This is Coleman's reinterpretation of Chabauty's idea for proving Mordell Conjecture (Faltings's theorem); for a long time it was the only significant progress on the conjecture.
Remark

The functions $f_i$ are locally analytic functions, and so $X(\mathbb{Q}_p)_1$, and thus $X(\mathbb{Q})$ is finite.

Within a residue disc, an integral $\int_P P' \omega = \int_{P(t)} P'(t) \omega(t) dt$ has a power series expansion in a uniformizer $t$.

Bound number of zeros with Newton polygon.
Remark

The functions $f_i$ are locally analytic functions, and so $X(\mathbb{Q}_p)_1$, and thus $X(\mathbb{Q})$ is finite.

Within a residue disc, an integral $\int_P P' \omega = \int_{P(t)} P'(t) \omega(t)dt$ has a power series expansion in a uniformizer $t$.

Bound number of zeros with Newton polygon.

Global bound: if $p > 2g$, then $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2)$. 
Remark

The functions $f_i$ are locally analytic functions, and so $X(\mathbb{Q}_p)_1$, and thus $X(\mathbb{Q})$ is finite.

Within a residue disc, an integral $\int_{P'} \omega = \int_{P(t)} P'(t) \omega(t) dt$ has a power series expansion in a uniformizer $t$.

Bound number of zeros with Newton polygon.

Global bound: if $p > 2g$, then $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2)$.

This is Coleman’s reinterpretation of Chabauty’s idea for proving Mordell Conjecture (Faltings’s theorem); for a long time it was the only significant progress on the conjecture.
Genus 2, rank 1 Chabauty-Coleman

Suppose $X$ is genus 2 hyperelliptic and rank $J(\mathbb{Q}) = 1$, $\infty \in X(\mathbb{Q})$. Fix $p$ of good reduction.

- Fix a basis for the differentials $dx/y, xdx/y$.
- Suppose we can find $P \in X(\mathbb{Q})$ of infinite order in $J(\mathbb{Q})$.

Compute $p$-adic numbers

$$\int_{\infty}^{P} dx/y = A, \int_{\infty}^{P} xdx/y = B,$$

and solve

$$X(\mathbb{Q}_p)_1 = \left\{ z \in X(\mathbb{Q}_p) : \int_{\infty}^{z} (Bdx/y - Axdx/y) = 0 \right\}.$$

Any $Q \in X(\mathbb{Q})$ is torsion or $nP$ for $n \in \mathbb{Q}$, and

$$\int_{\infty}^{nP} (Bdx/y - Axdx/y) = (BA - AB) = 0.$$
Genus 3, rank 0, hyperelliptic

\[ X : y^2 = x^7 - 37024x^6 + 3134464x^5 - 101220352x^4 + \\
1613758464x^3 - 13656653824x^2 + 59055800320x - 103079215104 \]
Genus 3, rank 0, hyperelliptic

\[ X : y^2 = x^7 - 37024x^6 + 3134464x^5 - 101220352x^4 + \\
1613758464x^3 - 13656653824x^2 + 59055800320x - 103079215104 \]

We write \( f_i(z) = \int_{\infty}^{z} \omega_i \) in local coordinates and find their zeros above each point of \( X(\mathbb{F}_7) \). Thus we prove \( X(\mathbb{Q}) = \{(32, 0), \infty\} \).
Genus 3, rank 0, hyperelliptic

\[ X : y^2 = x^7 - 37024x^6 + 3134464x^5 - 101220352x^4 + 1613758464x^3 - 13656653824x^2 + 59055800320x - 103079215104 \]

We write \( f_i(z) = \int_{\infty}^{z} \omega_i \) in local coordinates and find their zeros above each point of \( X(\mathbb{F}_7) \). Thus we prove \( X(\mathbb{Q}) = \{(32, 0), \infty\} \).

<table>
<thead>
<tr>
<th>disc</th>
<th>common roots of ( f_1(z) ), ( f_2(z) ) and ( f_3(z) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \infty )</td>
<td>( \infty )</td>
</tr>
<tr>
<td>( (0, \pm 4) )</td>
<td>no common roots</td>
</tr>
<tr>
<td>( (1, \pm 5) )</td>
<td>no common roots</td>
</tr>
<tr>
<td>( (2, \pm 6) )</td>
<td>no common roots</td>
</tr>
<tr>
<td>( (4, 0) )</td>
<td>( (32, 0) )</td>
</tr>
<tr>
<td>( (6, \pm 2) )</td>
<td>no common roots</td>
</tr>
</tbody>
</table>
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 - 3x^2 + x + 1 \]
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 - 3x^2 + x + 1 \]

Applying the algorithm at \( p = 11 \), we find \( X(\mathbb{Q}) = \{(0, 1), (1, 0), \infty\} \).
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 - 3x^2 + x + 1 \]

Applying the algorithm at \( p = 11 \), we find
\[ X(\mathbb{Q}) = \{(0, 1), (1, 0), \infty\}. \]
But if \( p = 5 \), there is an extra point: \( x = 2, y^3 = 7 \).
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 - 3x^2 + x + 1 \]

Applying the algorithm at \( p = 11 \), we find
\[ X(\mathbb{Q}) = \{(0,1), (1,0), \infty\}. \]
But if \( p = 5 \), there is an extra point: \( x = 2, y^3 = 7 \). It turns out that
\[ 3(2, 7^{1/3}) - \infty - 2(1,0) \]
is principal, so
\[ 3(2, 7^{1/3}) - 3\infty \simeq 2(1,0) - 2\infty \]
as divisors. Since \( (1,0) - \infty \) is 3-torsion, the extra solution is a 9-torsion point.
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 + x^3 - 3x^2 - 2x \]
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 + x^3 - 3x^2 - 2x \]

We compute rational points \( \{(0, 0), (2, 2), (-2, 0), (-1, -1), \infty\} \).
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 + x^3 - 3x^2 - 2x \]

We compute rational points \( \{(0, 0), (2, 2), (-2, 0), (-1, -1), \infty\} \).

Running Chabauty-Coleman at \( p = 7, 11, 13 \), returns the 7-adic point with \( x \)-coordinate \(-105237648 + O(7^{10})\), the 11-adic point with \( x \)-coordinate \(-800588 + O(11^6)\) and the 13-adic point \( 864 + O(13^3) \).
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 + x^3 - 3x^2 - 2x \]

We compute rational points \( \{(0, 0), (2, 2), (-2, 0), (-1, -1), \infty\} \).

Running Chabauty-Coleman at \( p = 7, 11, 13 \), returns the 7-adic point with \( x \)-coordinate \(-105237648 + O(7^{10})\), the 11-adic point with \( x \)-coordinate \(-800588 + O(11^6)\) and the 13-adic point \( 864 + O(13^3) \).

The \( x \)-coordinates come from a global point of \( X \), \((\alpha, \alpha^2 + 2\alpha)\), where \( \alpha \) is a root of \( x^3 + 3x^2 + 1 \).
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 + x^3 - 3x^2 - 2x \]

We compute rational points \{(0,0), (2,2), (-2,0), (-1,-1), \infty \}.

Running Chabauty-Coleman at \( p = 7, 11, 13 \), returns the 7-adic point with \( x \)-coordinate \(-105237648 + O(7^{10})\), the 11-adic point with \( x \)-coordinate \(-800588 + O(11^6)\) and the 13-adic point \(864 + O(13^3)\).

The \( x \)-coordinates come from a global point of \( X \), \((\alpha, \alpha^2 + 2\alpha)\), where \( \alpha \) is a root of \( x^3 + 3x^2 + 1 \).

The field \( \mathbb{Q}(\alpha) \) has a prime of degree 1 above 7,11, and 13 but not 17. Trying Chabauty-Coleman at \( p = 17 \) yields no extra points.
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 + x^3 - 3x^2 - 2x \]

We compute rational points \( \{(0,0), (2,2), (-2,0), (-1,-1), \infty\} \).

Running Chabauty-Coleman at \( p = 7, 11, 13 \), returns the 7-adic point with \( x \)-coordinate \(-105237648 + O(7^{10})\), the 11-adic point with \( x \)-coordinate \(-800588 + O(11^6)\) and the 13-adic point \(864 + O(13^3)\).

The \( x \)-coordinates come from a global point of \( X \), \((\alpha, \alpha^2 + 2\alpha)\), where \( \alpha \) is a root of \( x^3 + 3x^2 + 1 \).

The field \( \mathbb{Q}(\alpha) \) has a prime of degree 1 above 7,11, and 13 but not 17. Trying Chabauty-Coleman at \( p = 17 \) yields no extra points.

\( 3[(\alpha, \alpha^2 + 2\alpha) - \infty] \) is in \( J(\mathbb{Q}) \).
Our curves come from a database of genus 3 curves over $\mathbb{Q}$ of small discriminant computed by Drew Sutherland.
Our curves come from a database of genus 3 curves over \( \mathbb{Q} \) of small discriminant computed by Drew Sutherland.

He devised a method to “search the sky” (imagine looking at \( 10^{18} \) curves and picking only \( 10^5 \) interesting curves! you can’t even store all that data, \( \sim 100 \) exabytes).
Our curves come from a database of genus 3 curves over $\mathbb{Q}$ of small discriminant computed by Drew Sutherland.

He devised a method to “search the sky” (imagine looking at $10^{18}$ curves and picking only $10^5$ interesting curves! you can’t even store all that data, $\sim 100$ exabytes).

Also rely on magma implementation of Coleman integrals for general curves by Balakrishnan and Tuitman.
Our curves come from a database of genus 3 curves over $\mathbb{Q}$ of small discriminant computed by Drew Sutherland.

He devised a method to “search the sky” (imagine looking at $10^{18}$ curves and picking only $10^5$ interesting curves! you can’t even store all that data, $\sim 100$ exabytes).

Also rely on magma implementation of Coleman integrals for general curves by Balakrishnan and Tuitman.

We have provably computed rational points on over five thousand genus 3 rank 0 hyperelliptic curves, as well as a growing database of genus 3 rank 1 Picard curves.
Why compute data?

Data helps refine conjectures which then informs what data to compute.
Why compute data?

Data helps refine conjectures which then informs what data to compute.

Running algorithms on databases of curves tests all cases of those algorithms, catches bugs.
Beyond rational points

What if we don’t have a rational point which generates $J(\mathbb{Q})$?
Beyond rational points

What if we don’t have a rational point which generates $J(\mathbb{Q})$?

Fixing a rational base point $b$, there is a canonical map $Sym^g(X) \to J$ sending $(P_1, \ldots, P_g) \mapsto [P_1 + \cdots + P_g - gb]$. 

Generator for $J(\mathbb{Q})$ is a divisor defined over at most a degree $g$ extension of $\mathbb{Q}$. For example $X: y^3 - (x^4 + 7x^3 + 8x^2 - 15x + 4)$ has genus 3 rank 1, with generator $[(-2 + \sqrt{5}, 1) + (-2 - \sqrt{5}, 1) - 2\infty]$. The $x$-coordinates here are roots of $x^2 + 4x - 1$, and $p = 11$ splits completely in $L = \mathbb{Q}[x]/(x^2 + 4x - 1)$, so if $p | p$, $L_p \cong \mathbb{Q}_p$. Most of the time work locally in $\mathbb{Q}_p$. Modifications to code to handle divisors instead of points.
Beyond rational points

What if we don’t have a rational point which generates $J(\mathbb{Q})$?

Fixing a rational base point $b$, there is a canonical map $Sym^g(X) \rightarrow J$ sending $(P_1, \ldots, P_g) \mapsto [P_1 + \cdots + P_g - gb]$.

Generator for $J(\mathbb{Q})$ is a divisor defined over at most a degree $g$ extension of $\mathbb{Q}$. 

Databases of rational points

Sachi Hashimoto
Beyond rational points

What if we don’t have a rational point which generates $J(\mathbb{Q})$?

Fixing a rational base point $b$, there is a canonical map $\text{Sym}^g(X) \to J$ sending $(P_1, \ldots, P_g) \mapsto [P_1 + \cdots + P_g - gb]$.

Generator for $J(\mathbb{Q})$ is a divisor defined over at most a degree $g$ extension of $\mathbb{Q}$.

For example $X : y^3 - (x^4 + 7x^3 + 8x^2 - 15x + 4)$ has genus 3 rank 1, with generator $[(-2 + \sqrt{5}, 1) + (-2 - \sqrt{5}, 1) - 2\infty]$. The $x$-coordinates here are roots of $x^2 + 4x - 1$, and $p = 11$ splits completely in $L = \mathbb{Q}[x]/(x^2 + 4x - 1)$, so if $\mathfrak{p}|p$, $L_{\mathfrak{p}} \simeq \mathbb{Q}_p$. 
Beyond rational points

What if we don’t have a rational point which generates $J(\mathbb{Q})$?

Fixing a rational base point $b$, there is a canonical map $Sym^g(X) \to J$ sending $(P_1, \ldots, P_g) \mapsto [P_1 + \cdots + P_g - gb]$.

Generator for $J(\mathbb{Q})$ is a divisor defined over at most a degree $g$ extension of $\mathbb{Q}$.

For example $X : y^3 - (x^4 + 7x^3 + 8x^2 - 15x + 4)$ has genus 3 rank 1, with generator $[(-2 + \sqrt{5}, 1) + (-2 - \sqrt{5}, 1) - 2\infty]$. The $x$-coordinates here are roots of $x^2 + 4x - 1$, and $p = 11$ splits completely in $L = \mathbb{Q}[x]/(x^2 + 4x - 1)$, so if $p|p$, $L_p \simeq \mathbb{Q}_p$.

Most of the time work locally in $\mathbb{Q}_p$. Modifications to code to handle divisors instead of points.
Coleman gives a global bound for $p > 2g$ of
$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2).$$
Stoll improves upon this bound if, for example, $r' < g - 1$, showing
$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r'.$$
Coleman gives a global bound for $p > 2g$ of
\[ \#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2). \]
Stoll improves upon this bound if, for example, $r' < g - 1$, showing
\[ \#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r'. \]

$X : y^2 = x(x - 1)(x - 2)(x - 5)(x - 6)$ is a genus 2, rank 1 curve
with good reduction at 7 and $\#X(\mathbb{F}_7) = 8$. Coleman’s bound
implies $\#X(\mathbb{Q}) \leq 10$ and we can find 10 points, the Weierstrass
points along with $(3, \pm 6), (10 \pm 120)$ and $\infty$. 

Do other curves achieve the Coleman bound? (Note that Stoll
bound is sometimes an obstruction.)

Can you find one in genus 3? If not why?

Questions
Questions

Coleman gives a global bound for $p > 2g$ of

$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2)$. Stoll improves upon this bound if, for example, $r' < g - 1$, showing $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r'$.

$X : y^2 = x(x - 1)(x - 2)(x - 5)(x - 6)$ is a genus 2, rank 1 curve with good reduction at 7 and $\#X(\mathbb{F}_7) = 8$. Coleman’s bound implies $\#X(\mathbb{Q}) \leq 10$ and we can find 10 points, the Weierstrass points along with $(3, \pm 6), (10 \pm 120)$ and $\infty$.

Do other curves achieve the Coleman bound? (Note that Stoll bound is sometimes an obstruction.)
Questions

Coleman gives a global bound for $p > 2g$ of
$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2).$$
Stoll improves upon this bound if, for example, $r' < g - 1$, showing
$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r'.$$

$X : y^2 = x(x - 1)(x - 2)(x - 5)(x - 6)$ is a genus 2, rank 1 curve with good reduction at 7 and $\#X(\mathbb{F}_7) = 8$. Coleman’s bound implies $\#X(\mathbb{Q}) \leq 10$ and we can find 10 points, the Weierstrass points along with $(3, \pm 6), (10 \pm 120)$ and $\infty$.

Do other curves achieve the Coleman bound? (Note that Stoll bound is sometimes an obstruction.)

Can you find one in genus 3? If not why?